N° 85-002-X au catalogue
ISSN 1205-8882

Juristat

Les cybercrimes déclarés par la police au Canada, 2012

par Benjamin Mazowita et Mireille Vézina

Date de diffusion : le 25 septembre 2014

Statistique Canada Statistics Canada

Canada

Comment obtenir d'autres renseignements

Pour toute demande de renseignements au sujet de ce produit ou sur l'ensemble des données et des services de Statistique Canada, visiter notre site Web à www.statcan.gc.ca.

Vous pouvez également communiquer avec nous par :

Courriel à infostats@statcan.gc.ca

Téléphone entre 8 h 30 et 16 h 30 du lundi au vendredi aux numéros sans frais suivants :

- Service de renseignements statistiques 1-800-263-1136
- Service national d'appareils de télécommunications pour les malentendants 1-800-363-7629
- Télécopieur 1-877-287-4369

Programme des services de dépôt

- Service de renseignements 1-800-635-7943
- Télécopieur 1-800-565-7757

Comment accéder à ce produit

Le produit n° 85-002-X au catalogue est disponible gratuitement sous format électronique. Pour obtenir un exemplaire, il suffit de visiter notre site Web à www.statcan.gc.ca et de parcourir par « Ressource clé » > « Publications ».

Normes de service à la clientèle

Statistique Canada s'engage à fournir à ses clients des services rapides, fiables et courtois. À cet égard, notre organisme s'est doté de normes de service à la clientèle que les employés observent. Pour obtenir une copie de ces normes de service, veuillez communiquer avec Statistique Canada au numéro sans frais 1-800-263-1136. Les normes de service sont aussi publiées sur le site www.statcan.gc.ca sous « À propos de nous » > « Notre organisme » > « Offrir des services aux Canadiens ».

Publication autorisée par le ministre responsable de Statistique Canada

© Ministre de l'Industrie, 2014

Tous droits réservés. L'utilisation de la présente publication est assujettie aux modalités de l'entente de licence ouverte de Statistique Canada (www.statcan.gc.ca/reference/licence-fra.htm).

This publication is also available in English.

Note de reconnaissance

Le succès du système statistique du Canada repose sur un partenariat bien établi entre Statistique Canada et la population du Canada, ses entreprises, ses administrations et les autres établissements. Sans cette collaboration et cette bonne volonté, il serait impossible de produire des statistiques exactes et actuelles.

Signes conventionnels

Les signes conventionnels suivants sont employés dans les publications de Statistique Canada :

.	indisponible pour toute période de référence
..	indisponible pour une période de référence précise
...	n'ayant pas lieu de figurer
0	zéro absolu ou valeur arrondie à zéro
0^s	valeur arrondie à 0 (zéro) là où il y a une distinction importante entre le zéro absolu et la valeur arrondie
^{p}	provisoire
^{r}	révisé
x	confidentiel en vertu des dispositions de la *Loi sur la statistique*
^{E}	à utiliser avec prudence
F	trop peu fiable pour être publié
*	valeur significativement différente de l'estimation pour la catégorie de référence ($p<0,05$)

Les cybercrimes déclarés par la police au Canada, 2012: faits saillants

- En 2012, 9 084 affaires de cybercriminalité ont été déclarées par certains services de police desservant 80 % de la population du Canada. Ce chiffre représentait un taux de 33 affaires de cybercriminalité pour chaque tranche de 100 000 habitants.
- Le type de cybercrime le plus courant était la fraude, représentant plus de la moitié (54 %) de tous les cybercrimes déclarés par la police en 2012. Les infractions liées à l'intimidation, composées de celles où il y a des menaces de violence, constituaient 20 % des cybercrimes déclarés par la police en 2012, alors que 16 % des cybercrimes comportaient une infraction cybernétique de nature sexuelle.
- En 2012, un auteur présumé a été identifié par la police dans une proportion relativement faible (6 %) des cybercrimes contre les biens, notamment dans des affaires de fraude (5 %) et de vol d'identité (3 %).
- Un auteur présumé a été identifié par la police relativement à 31 % des infractions cybernétiques de nature sexuelle et 55 % des cybercrimes liés à des affaires d'intimidation. Comparativement aux infractions liées à l'intimidation, les infractions sexuelles étaient plus souvent classées par mise en accusation (25 % par rapport à 18 %).
- La majorité (76 %) des auteurs présumés identifiés par la police en 2012 étaient des hommes. Dans le cas des infractions cybernétiques de nature sexuelle, les hommes représentaient 94 % des auteurs présumés.
- Les auteurs présumés identifiés par la police relativement à des infractions liées à l'intimidation avaient tendance à être jeunes, plus du quart (28 %) ayant moins de 18 ans, tandis que les auteurs présumés de cybercrimes de nature sexuelle étaient généralement un peu plus vieux, puisque la plus grande proportion (22 %) des auteurs présumés de cybercrimes de nature sexuelle étaient âgés de 25 à 34 ans.
- Les services de police ont identifié 2 070 victimes d'actes de violence comportant un cybercrime en 2012. Les femmes représentaient la majorité des victimes d'actes de violence liés à un cybercrime (69 %), surtout dans les affaires comportant une infraction sexuelle (84 %).
- Dans l'ensemble, 42 % des victimes de cybercrimes déclarés par la police avaient moins de 18 ans. En 2012, presque toutes (96 %) les victimes d'infractions sexuelles liées à un cybercrime étaient âgées de moins de 18 ans, dont 10 % avaient moins de 12 ans.
- La plupart (73 %) des victimes d'affaires de violence liées à un cybercrime connaissaient l'auteur présumé. Les victimes d'infractions sexuelles comportant un cybercrime étaient moins susceptibles de connaitre l'auteur présumé (57 %), comparativement aux victimes d'infractions avec violence de nature non sexuelle (77 %).
- Selon les résultats de l'Enquête sociale générale de 2009 sur la victimisation, environ 1,75 million de Canadiens de 15 ans et plus ont mentionné avoir été victimes de cyberintimidation. Cela représentait 8 % des utilisateurs d'Internet âgés de 15 ans et plus. Moins de 1 victime de cyberintimidation sur 10 (7 %) a signalé l'incident à la police.

Les cybercrimes déclarés par la police au Canada, 2012

par Benjamin Mazowita et Mireille Vézina

Internet fait de plus en plus partie intégrante de la vie quotidienne des Canadiens. Selon les résultats de l'Enquête canadienne sur l'utilisation d'Internet, 83 % des Canadiens âgés de 16 ans et plus ont utilisé Internet à des fins personnelles en 2012. La majorité des utilisateurs d'Internet au Canada ont effectué des opérations bancaires en ligne (72 %), visité des sites de réseautage social (67 %) et commandé des biens et services en ligne (56 %). La valeur totale des commandes passées en ligne par les Canadiens s'établissait à 18,9 milliards de dollars en 2012 (Statistique Canada, 2013).

La croissance rapide de l'utilisation d'Internet a permis l'émergence de nouvelles occasions de perpétrer des crimes (Nuth, 2008). Les infractions criminelles pour lesquelles un ordinateur ou Internet est la cible d'un crime ou un instrument employé pour perpétrer un crime sont désignées collectivement par les termes « cybercrimes » ou « cybercriminalité » (voir l'encadré 1). La fraude, le vol d'identité, l'extorsion, le harcèlement criminel, certaines infractions sexuelles et les infractions de pornographie juvénile font partie des infractions criminelles qui peuvent être perpétrées sur Internet au moyen d'un ordinateur, d'une tablette ou d'un téléphone intelligent.

À l'aide des données du Programme de déclaration uniforme de la criminalité fondé sur l'affaire (version 2.2) de 2012, le présent article du *Juristat* traite des cybercrimes déclarés par la police au Canada[1,2]. L'analyse porte sur le nombre de cybercrimes déclarés par les services de police desservant 80 % de la population du Canada ainsi que sur les caractéristiques des affaires, des victimes et des auteurs présumés d'infractions cybernétiques. Ces constatations s'accompagnent des données autodéclarées sur la cyberintimidation, à partir des résultats de l'Enquête sociale générale de 2009 sur la victimisation.

Les cybercrimes déclarés par la police

Encadré 1
Définition et mesure des cybercrimes déclarés par la police

Définition

La cybercriminalité est un phénomène complexe et ses caractéristiques non conventionnelles posent bien des défis aux services de police et au système de justice pénale dans l'ensemble. Le manque de renseignements fiables sur la cybercriminalité a été désigné comme un obstacle majeur à l'élaboration de stratégies de prévention du crime portant sur la cybercriminalité (Smyth et Carleton, 2011).

Pour recueillir des statistiques fiables sur la cybercriminalité, il faut disposer d'une définition normalisée. Le Programme de déclaration uniforme de la criminalité (DUC) a adopté la définition de la cybercriminalité établie par le Collège canadien de police : « Les infractions criminelles ayant l'ordinateur pour objet ou pour instrument de perpétration principal » (Kowalski, 2002). On peut donc diviser la cybercriminalité en deux grandes catégories : les affaires pour lesquelles l'ordinateur ou Internet est la **cible** d'un crime, comme le piratage informatique et l'utilisation non autorisée de systèmes informatiques, et celles pour lesquelles un ordinateur ou Internet est l'**instrument** utilisé pour perpétrer un crime, comme le leurre d'enfants au moyen d'un ordinateur ou une fraude perpétrée sur Internet (Centre canadien de la statistique juridique, 2013). En 2012, les services de police ont fait savoir que, dans 88 % des cybercrimes signalés, un ordinateur ou Internet avait été l'instrument utilisé pour perpétrer une infraction, alors que dans 10 % des cas, un ordinateur ou Internet avait été la cible de l'infraction. Le genre de cybercrime ne pouvait être déterminé pour les autres affaires (2 %).

Encadré 1 suite
Définition et mesure des cybercrimes déclarés par la police

Données fondées sur l'affaire

Des services de police desservant 80 % de la population du Canada ont déclaré des données sur la cybercriminalité au Centre canadien de la statistique juridique en 2012 dans le cadre du Programme DUC fondé sur l'affaire (version 2.2)[3]. Une affaire criminelle peut comporter de nombreuses infractions. Au moment de déclarer des données au Programme DUC, la police peut indiquer jusqu'à quatre infractions dans une seule affaire. Pour assurer l'uniformité de la déclaration au fil du temps et entre les services de police, les affaires criminelles déclarées par la police sont dénombrées en fonction de l'**infraction la plus grave** dans l'affaire. Néanmoins, pour analyser les affaires de cybercriminalité, une infraction précise dans une affaire a été identifiée comme l'**infraction cybernétique**. Cette dernière représente l'infraction criminelle particulière dans une affaire où un ordinateur ou Internet était la cible du crime ou a constitué l'instrument de perpétration du crime. Bien que, dans la majorité (99 %) des affaires de cybercriminalité, l'infraction cybernétique soit l'infraction la plus grave dans l'affaire, ce n'est pas le cas pour un petit nombre d'affaires de cybercriminalité. Par exemple, dans une affaire comportant à la fois l'envoi de courriels menaçants et des voies de fait, l'infraction cybernétique serait la profération de menaces, tandis que l'infraction la plus grave dans l'affaire serait les voies de fait. Pour en savoir plus sur les affaires de cybercriminalité pour lesquelles l'infraction cybernétique n'est pas l'infraction la plus grave dans l'affaire, voir l'encadré 3.

Aux fins de la présente analyse, les constatations liées aux caractéristiques des affaires de cybercriminalité et des auteurs présumés de ce type de crime sont présentées en fonction de l'**infraction cybernétique**. En revanche, l'analyse des victimes de cybercriminalité est présentée selon l'**infraction commise contre la victime**, pour que l'on puisse déterminer l'infraction la plus grave commise à l'endroit de chaque victime.

La fraude représente plus de la moitié des affaires de cybercriminalité déclarées par la police

En 2012, 9 084 affaires de cybercriminalité ont été déclarées par les services de police desservant 80 % de la population du Canada. Cela représentait un taux de 33 affaires de cybercriminalité pour chaque tranche de 100 000 habitants[4] (tableau 1).

Les infractions contre les biens constituaient la majorité (61 %) des affaires de cybercriminalité en 2012, soit 5 544 affaires. À elle seule, la fraude[5] représentait plus de la moitié (54 %) des cybercrimes corroborés par la police. Parmi les autres cybercrimes contre les biens dignes de mention, on trouve la fraude d'identité (5 %), le méfait (2 %) et le vol d'identité (1 %)[6].

Graphique 1
Affaires de cybercriminalité déclarées par la police, selon le type d'infraction, certains services de police, 2012

1. Comprend le vol d'identité et le trafic de biens volés.
2. Comprend l'intimidation d'une personne associée au système judiciaire ou d'un journaliste et l'intimidation d'une personne qui n'est pas associée au système judiciaire.
3. Comprend le voyeurisme, l'exploitation sexuelle, la corruption d'enfants, le fait de rendre accessible à un enfant du matériel sexuellement explicite et la bestialité — la perpétration ou l'usage de la force.
4. Comprend la traite de personnes et d'autres infractions avec violence.
5. Comprend des infractions telles que la corruption des mœurs, les actions indécentes, les infractions contre la personne et la réputation, le défaut de se conformer à une ordonnance et le manquement aux conditions de la probation.

Note: Les renseignements qui figurent dans le présent tableau reflètent les données déclarées par les services de police desservant 80 % de la population du Canada.

Source : Statistique Canada, Centre canadien de la statistique juridique, Programme de déclaration uniforme de la criminalité fondé sur l'affaire.

En 2012, les services de police ont déclaré 3 284 affaires criminelles dans lesquelles l'infraction cybernétique était une infraction contre la personne[7], ce qui représentait 36 % des cybercrimes signalés. Aux fins de la présente analyse, les cybercrimes contre la personne se répartissent en deux catégories distinctes : les **infractions liées à l'intimidation**, qui comprennent les menaces de violence, le harcèlement criminel et l'extorsion; et les **infractions sexuelles**, notamment le leurre d'enfants au moyen d'un ordinateur et les infractions de pornographie juvénile. Pour obtenir la liste complète des infractions qui font partie de chaque catégorie, voir le tableau 1.

Les infractions liées à l'intimidation représentaient 1 cybercrime déclaré par la police sur 5 (20 %) en 2012, ce qui correspond à 1 839 affaires. Les menaces et le harcèlement criminel, qui constituaient 8 % et 6 % respectivement des cybercrimes déclarés, étaient les infractions liées à l'intimidation les plus courantes.

En 2012, la police a déclaré 1 441 affaires de cybercriminalité pour lesquelles l'infraction cybernétique était une infraction sexuelle; cela représentait 16 % des cybercrimes déclarés par la police. Le leurre d'enfants au moyen d'un ordinateur[8] constituait une part importante des infractions cybernétiques de nature sexuelle et représentait 6 % des cybercrimes déclarés par la police. Par ailleurs, les infractions de pornographie juvénile[9], — qui comprennent l'accès à de la pornographie juvénile de même que la possession, la production et la distribution de cette pornographie — représentaient 9 % des cybercrimes déclarés par la police. En 2012, dans 805 affaires de cybercriminalité ayant fait l'objet d'une enquête par certains services de police au Canada, l'infraction cybernétique était liée à de la pornographie juvénile.

Par ailleurs, 3 % des affaires de cybercriminalité étaient d'autres infractions au *Code criminel*, notamment la corruption des mœurs, les actions indécentes et les infractions contre la personne et la réputation.

Encadré 2
Les cybercrimes portés à l'attention de la police

Le signalement des cybercrimes à la police peut dépendre de divers facteurs. Comme pour les crimes déclarés par les services de police de façon plus générale, la collecte et la déclaration de statistiques peuvent être influencées par les procédures des services de police locaux, les perceptions du public et la volonté d'une personne de signaler à la police qu'elle a été victime, ainsi que par divers facteurs législatifs et sociaux (Brennan, 2012).

La détection de la cybercriminalité par la police peut être influencée par les ressources dont disposent les services de police locaux sur le terrain. Par exemple, l'existence d'une équipe responsable de la cybercriminalité au sein d'un service de police se répercute sur la capacité de ce dernier de déceler les cybercrimes et d'enquêter sur ceux-ci. Ainsi, les données peuvent indiquer, en partie, les différences dans les ressources et stratégies qu'emploient les services de police pour déceler les cybercrimes.

Selon la police, les percées technologiques, notamment la prolifération des téléphones intelligents, les réseaux en ligne anonymes, les systèmes de devises virtuelles et l'informatique en nuage, ont créé de nouvelles possibilités pour les criminels et nécessitent des mesures policières innovatrices (Gendarmerie royale du Canada, 2014).

En outre, les caractéristiques spatiales irrégulières de la cybercriminalité posent des obstacles particuliers en ce qui concerne l'identification des affaires de cybercriminalité et l'enquête sur ces affaires. Contrairement aux délits plus conventionnels, de nombreux cybercrimes ne peuvent être rattachés à des limites géographiques précises. Les cybercrimes peuvent être commis à distance et sur des réseaux virtuels décentralisés, traversant les frontières provinciales et nationales. Les données déclarées par la police indiquent le secteur de compétence où l'infraction a été signalée et consignée, mais pas nécessairement celui où l'incident ou la victimisation s'est produit. Les lois, ressources et activités consacrées à la lutte contre la cybercriminalité peuvent varier d'un secteur de compétence à l'autre et dans le temps, ce qui se répercute sur le nombre de cybercrimes qui sont signalés à la police. Étant donné la nature bien particulière de la cybercriminalité, il n'est pas recommandé de faire des comparaisons dans le temps ou entre des secteurs de compétence.

Il y a plus de chances qu'un auteur présumé soit identifié dans des affaires de cybercriminalité contre la personne

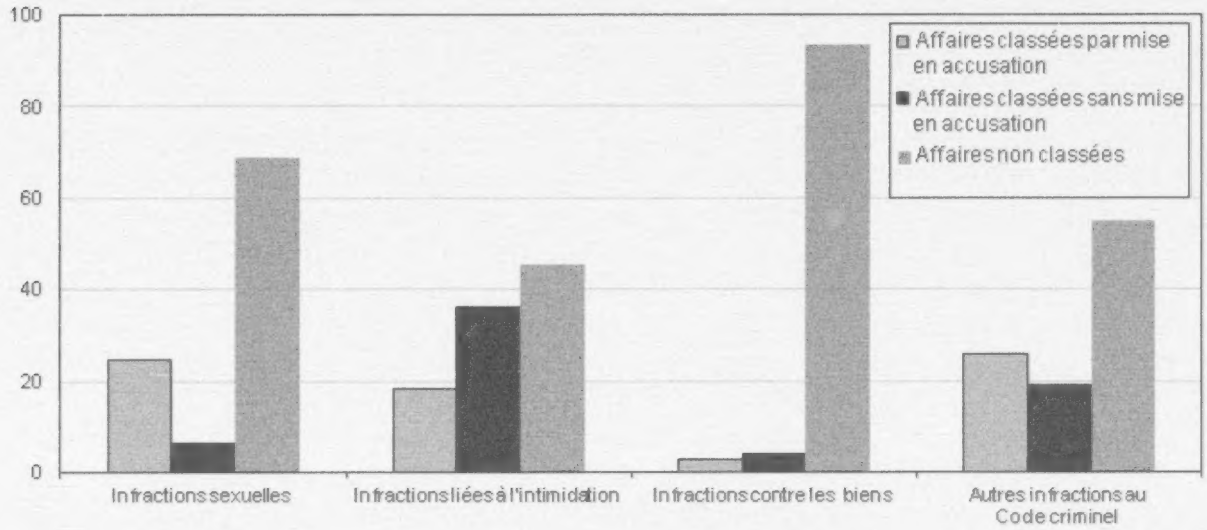
Un auteur présumé a été identifié dans 21 % des affaires de cybercriminalité déclarées par la police en 2012, ce qui signifie que les autres affaires de cybercriminalité portées à l'attention de la police cette année-là (79 %) n'ont pas été classées[10] (tableau 2).

En 2012, 6 % des cybercrimes contre les biens ont été classés soit par mise en accusation, soit sans mise en accusation. Le faible taux de classement des cybercrimes contre les biens s'explique par le fait qu'un auteur présumé a été identifié dans seulement une petite proportion d'affaires de fraude (5 %) et de vol d'identité (3 %).

En revanche, 31 % des infractions cybernétiques de nature sexuelle et 55 % des cybercrimes liés à des affaires d'intimidation ont été classés soit par mise en accusation, soit sans mise en accusation en 2012 (graphique 2). Le taux de classement des cybercrimes de nature sexuelle a été influencé par le fait qu'un auteur présumé a été identifié dans seulement 23 % des affaires de pornographie juvénile, qui est l'infraction cybernétique de nature sexuelle la plus courante.

Graphique 2
Affaires de cybercriminalité déclarées par la police, selon le type d'infraction et l'état de classement des affaires, certains services de police, 2012

pourcentage



Note: Les renseignements qui figurent dans le présent graphique reflètent les données déclarées par les services de police desservant 80 % de la population du Canada. Pour qu'une affaire soit classée, il faut qu'un auteur présumé soit identifié et que les preuves soient suffisantes pour que des accusations soient portées en lien avec l'affaire. Les affaires peuvent être classées par mise en accusation ou par d'autres moyens (p. ex. sans mise en accusation). La catégorie « Infractions sexuelles » comprend les infractions sexuelles contre la personne et les infractions de pornographie juvénile. La catégorie « Infractions liées à l'intimidation » comprend les infractions contre la personne comportant des menaces de violence. La catégorie « Infractions contre les biens » comprend la fraude, le vol d'identité, la fraude d'identité, le méfait et le trafic de biens volés. La catégorie « Autres infractions au *Code criminel* » comprend des infractions telles que la corruption des mœurs, les actions indécentes et les infractions contre la personne et la réputation. Un petit nombre d'affaires classées dans les autres infractions avec violence est exclu du présent graphique. Voir le tableau 1 pour obtenir la liste des infractions qui font partie de chaque catégorie d'infractions.
Source : Statistique Canada, Centre canadien de la statistique juridique, Programme de déclaration uniforme de la criminalité fondé sur l'affaire.

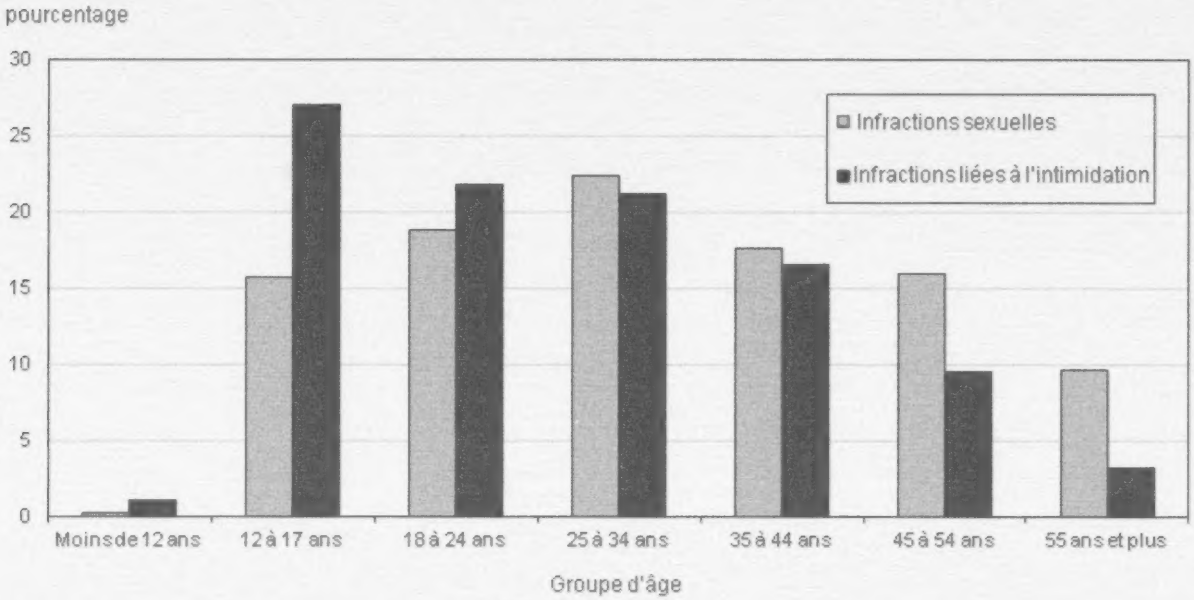
Comparativement aux infractions liées à l'intimidation, les cybercrimes de nature sexuelle étaient plus souvent classés par mise en accusation (25 % par rapport à 18 %). Cela s'explique par le fait que plusieurs infractions liées à l'intimidation, tout spécialement les menaces et le harcèlement criminel, ont été classées sans mise en accusation. Dans ces infractions, l'auteur présumé n'était pas souvent inculpé parce que le service de police exerçait son pouvoir discrétionnaire ou que le plaignant refusait de déposer des accusations.

La majorité des auteurs présumés de cybercrimes déclarés par la police sont des hommes

En 2012, les services de police ont identifié 2 051 auteurs présumés d'affaires de cybercriminalité (tableau 3). La majorité (76 %) d'entre eux étaient des hommes, dont ceux âgés de 18 à 34 ans représentaient 37 % des auteurs présumés de cybercrimes déclarés par la police cette année-là. La tendance chez les auteurs présumés de cybercrimes à être des hommes était particulièrement marquée dans le cas des infractions de nature sexuelle, pour lesquelles ils constituaient 94 % des auteurs présumés identifiés par la police.

Les auteurs présumés identifiés par la police relativement à des infractions liées à l'intimidation étaient généralement plus jeunes que les auteurs présumés de cybercrimes de nature sexuelle (graphique 3). Plus du quart (28 %) des auteurs présumés d'infractions liées à l'intimidation avaient moins de 18 ans, leur proportion diminuant avec l'âge. Par contre, la plus grande proportion (22 %) des auteurs présumés de cybercrimes de nature sexuelle étaient âgés de 25 à 34 ans, et 16 % des auteurs présumés identifiés relativement à des affaires de pornographie juvénile, qui constituait l'infraction cybernétique de nature sexuelle la plus courante, étaient âgés de 55 ans et plus.

Graphique 3
Répartition selon l'âge des auteurs présumés d'infractions cybernétiques contre la personne, selon les infractions sexuelles et les infractions liées à l'intimidation, certains services de police, 2012



Note: Les renseignements qui figurent dans le présent graphique reflètent les données déclarées par les services de police desservant 80 % de la population du Canada. Le nombre d'auteurs présumés est fondé sur l'infraction cybernétique dans l'affaire. La catégorie « Infractions sexuelles » comprend les infractions sexuelles contre la personne et les infractions de pornographie juvénile. La catégorie « Infractions liées à l'intimidation » comprend les infractions contre la personne comportant des menaces de violence. Les enregistrements relatifs aux auteurs présumés sont exclus lorsque l'âge ou le sexe est inconnu. Voir le tableau 1 pour obtenir la liste des infractions qui font partie de chaque catégorie d'infractions.
Source : Statistique Canada, Centre canadien de la statistique juridique, Programme de déclaration uniforme de la criminalité fondé sur l'affaire.

Les auteurs présumés de cybercrimes contre les biens étaient plus souvent âgés de 18 ans et plus; les hommes et les femmes adultes représentaient 67 % et 24 % respectivement des auteurs présumés. Environ 4 auteurs présumés sur 10 (41 %) identifiés par la police relativement à un cybercrime contre les biens étaient âgés de 25 à 34 ans.

Encadré 3
Un petit nombre de cybercrimes déclarés par la police sont commis conjointement avec une infraction plus grave

Une affaire criminelle peut se composer de plusieurs infractions. Au moment de déclarer des données au Programme de déclaration uniforme de la criminalité, la police peut indiquer jusqu'à quatre infractions dans une seule affaire. En général, lorsqu'une affaire comporte plusieurs infractions criminelles, elle est classée en fonction de l'infraction la plus grave dans l'affaire selon les règles d'enquête standards. Toutefois, pour analyser les données sur la cybercriminalité, une infraction dans l'affaire a été identifiée comme étant l'infraction cybernétique. L'infraction la plus grave et l'infraction cybernétique ne sont pas nécessairement la même. Bien que l'analyse des affaires présentées dans cet article de *Juristat* repose sur l'infraction cybernétique, cet encadré fournit des précisions sur les affaires qui comportent également une infraction plus grave.

En 2012, l'infraction cybernétique et l'infraction la plus grave dans l'affaire étaient la même dans presque toutes les affaires de cybercriminalité (99 %). La proportion restante de 1 % représentait 110 affaires de cybercriminalité pour lesquelles l'infraction cybernétique n'était pas l'infraction la plus grave dans l'affaire.

En 2012, on a dénombré 71 affaires de cybercriminalité (impliquant 87 victimes) qui comportaient également une agression sexuelle ou des contacts sexuels, et 26 affaires (impliquant 30 victimes) qui comprenaient des voies de fait.

Encadré 3 suite

Un petit nombre de cybercrimes déclarés par la police sont commis conjointement avec une infraction plus grave

La présence d'une infraction avec violence plus grave dans l'affaire est digne de mention dans plusieurs infractions cybernétiques. En 2012, 20 affaires sur 67 pour lesquelles l'infraction cybernétique était une incitation à des contacts sexuels comportaient aussi une infraction plus grave d'agression sexuelle ou de contacts sexuels. De même, parmi les 543 affaires pour lesquelles l'infraction cybernétique était le leurre d'enfants au moyen d'un ordinateur, 33 comprenaient également une infraction plus grave d'agression sexuelle ou de contacts sexuels.

Dans le cas des cybercrimes associés à des infractions liées à l'intimidation, 17 affaires de menaces sur 759 et 12 affaires de harcèlement criminel sur 560 comportaient une infraction avec violence plus grave dans l'affaire, notamment l'agression sexuelle, les voies de fait et la séquestration.

Un auteur présumé était plus susceptible d'être identifié dans des affaires de cybercriminalité liées à une infraction plus grave. En 2012, 82 % des affaires de cybercriminalité qui comportaient une infraction plus grave que l'infraction cybernétique ont été classées par mise en accusation, alors que 8 % ont été classées sans mise en accusation. Les affaires de cybercriminalité qui comportaient une infraction avec violence plus grave, comme une agression sexuelle ou des voies de fait, étaient également plus susceptibles de mettre en cause un auteur présumé connu de la victime. Les victimes d'agressions sexuelles ou de contacts sexuels associés à un cybercrime étaient plus communément la cible d'un ami ou d'une connaissance (56 %), tandis que les victimes de voies de fait associées à un cybercrime étaient plus souvent victimisées par un partenaire intime actuel ou ancien (55 %).

La plupart des victimes identifiées dans les affaires de violence comportant un cybercrime sont des femmes

En 2012, les services de police ont identifié 2 070 victimes d'affaires de violence comportant une infraction cybernétique[11] (tableau 4). Cela comprend 468 victimes d'infractions sexuelles et 1 602 victimes d'infractions avec violence de nature non sexuelle[12].

Un peu plus des deux tiers (69 %) des victimes d'affaires de cybercriminalité étaient des femmes. Ces dernières représentaient 84 % des victimes d'infractions sexuelles associées à un cybercrime et 65 % des victimes d'infractions avec violence de nature non sexuelle.

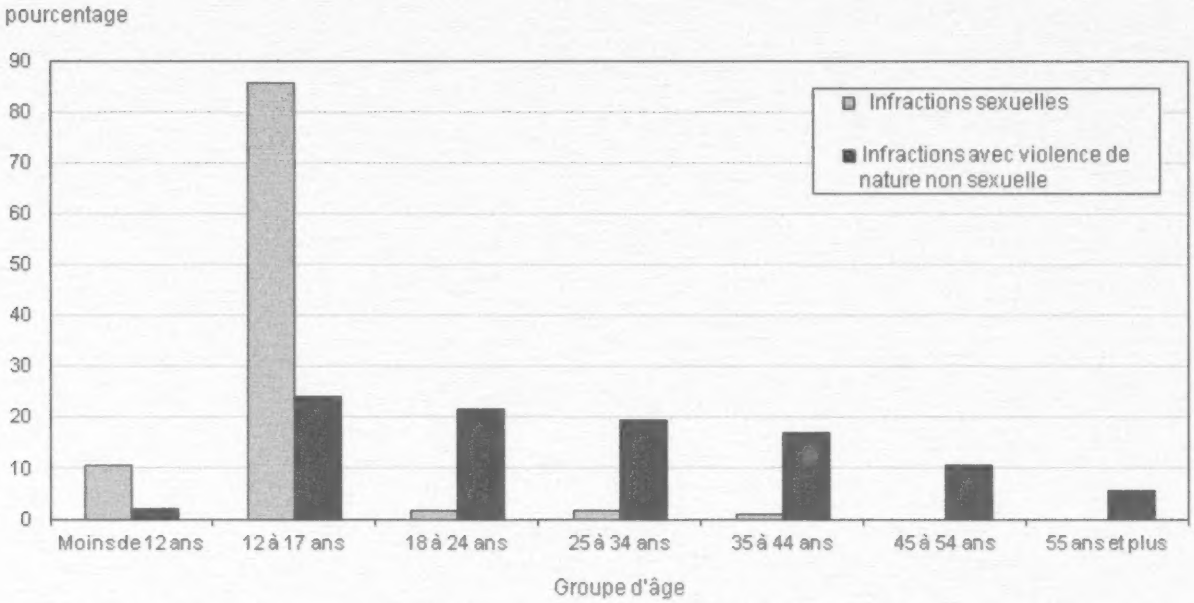
Les victimes d'affaires de violence comportant un cybercrime ont tendance à être jeunes

Les victimes de cybercrimes déclarés par la police sont généralement jeunes. Dans l'ensemble, 42 % des victimes de cybercrimes identifiées par la police étaient âgées de 17 ans et moins, alors que 17 % d'entre elles étaient âgées de 18 à 24 ans.

La prévalence des victimes de moins de 18 ans est particulièrement marquée dans les cas d'infractions de nature sexuelle (graphique 4). En 2012, 96 % de ces victimes étaient âgées de 17 ans et moins, y compris 10 % qui avaient moins de 12 ans. Les infractions cybernétiques de nature sexuelle courantes — notamment l'incitation à des contacts sexuels et le leurre d'enfants au moyen d'un ordinateur — sont des infractions sexuelles qui ciblent expressément les enfants.

Selon des analyses antérieures des données déclarées par la police réalisées au Canada, les jeunes représentent un nombre disproportionné de victimes d'infractions sexuelles. En 2012, les enfants et les jeunes représentaient 55 % des victimes de toutes les infractions sexuelles déclarées par la police, mais ils ne constituaient que 20 % de la population du Canada (Cotter et Beaupré, 2014).

Graphique 4
Répartition selon l'âge des victimes d'infractions avec violence liées à un cybercrime, selon les infractions sexuelles et les infractions avec violence de nature non sexuelle, certains services de police, 2012



Note: Les renseignements qui figurent dans le présent graphique reflètent les données déclarées par les services de police desservant 80 % de la population du Canada. Le nombre de victimes est fondé sur l'infraction commise contre la victime. La catégorie « Infractions sexuelles » comprend les infractions sexuelles contre la personne pour lesquelles les renseignements sur la victime ont été recueillis. La catégorie « Infractions avec violence de nature non sexuelle » comprend les voies de fait, les infractions contre la personne comportant des menaces de violence, et d'autres infractions avec violence. Les enregistrements relatifs aux victimes sont exclus lorsque l'âge ou le sexe est inconnu. Voir le tableau 5 pour obtenir la liste des infractions qui font partie de chaque catégorie d'infractions.
Source : Statistique Canada, Centre canadien de la statistique juridique, Programme de déclaration uniforme de la criminalité fondé sur l'affaire.

Par rapport aux infractions avec violence de nature sexuelle, les victimes d'infractions avec violence de nature non sexuelle associées à un cybercrime avaient tendance à être un peu plus vieilles. Environ le quart (26 %) des victimes étaient âgées de 17 ans ou moins, alors que la proportion restante de 74 % était âgée de 18 ans et plus.

En général, les victimes d'infractions avec violence liées à un cybercrime connaissent l'auteur présumé

Près des trois quarts (73 %) des victimes d'une infraction avec violence liée à un cybercrime déclaré par la police connaissaient l'auteur présumé (tableau 5). Dans la majorité des affaires, l'auteur présumé était un ami ou une connaissance (45 %), un partenaire intime actuel ou ancien (24 %) ou un membre de la famille (5 %) de la victime. Un peu plus du quart (27 %) des victimes ne connaissaient pas l'auteur présumé[13].

Par rapport aux infractions avec violence de nature non sexuelle, les victimes d'infractions sexuelles associées à un cybercrime étaient moins susceptibles de connaître l'auteur présumé. Environ 6 victimes d'infractions sexuelles sur 10 (57 %) connaissaient l'auteur présumé, qui était le plus souvent un ami ou une connaissance (45 %). La proportion restante de 43 % des victimes d'infractions sexuelles associées à un cybercrime ne connaissaient pas l'auteur présumé. L'agresseur était un étranger pour la majorité (55 %) des victimes d'infractions de leurre d'enfants au moyen d'un ordinateur, l'infraction avec violence de nature sexuelle la plus courante associée aux cybercrimes.

Dans les affaires de cybercriminalité comportant une infraction avec violence de nature non sexuelle, l'auteur présumé était plus susceptible d'être un ami ou une connaissance (44 %), ou encore un partenaire intime actuel ou ancien (28 %). Plus particulièrement, les victimes de harcèlement criminel avaient, en plus grand nombre, identifié l'auteur présumé comme un partenaire intime actuel ou ancien (47 %), plus souvent un ancien partenaire amoureux (32 %). Les victimes d'appels téléphoniques menaçants ou harcelants étaient plus susceptibles d'être la cible d'un ami ou d'une connaissance (44 %), alors que plus de la moitié des victimes d'extorsion ne connaissaient pas l'auteur présumé (60 %).

Encadré 4
Autres sources de données

Les données sur les cybercrimes déclarés par la police représentent les cybercrimes qui ont été portés à l'attention de celle-ci. Il est possible qu'il s'agisse d'une sous-estimation de la victimisation des Canadiens sur Internet. Par exemple, bien qu'ils constituent une proportion importante des cybercrimes déclarés à la police, bien des cas de fraude par Internet et de vol d'identité en ligne ne sont pas signalés à la police ou ne sont pas portés à son attention (Smyth et Carleton, 2011). Selon les résultats de l'Enquête sociale générale de 2009 sur la victimisation, 4 % des utilisateurs d'Internet ont été victimes de fraude bancaire au cours des 12 mois ayant précédé la tenue de l'enquête (Perreault, 2011).

Outre les données obtenues auprès des services de police et les données sur la victimisation, plusieurs organismes privés et publics recueillent et communiquent des données sur l'incidence de la cybercriminalité au Canada. Les types de données recueillies et les méthodes employées varient selon le mandat de chaque organisme et le domaine où il opère. Dans certains cas, les renseignements proviennent directement des déclarations du public, alors que dans d'autres cas, les données sont recueillies au moyen d'enquêtes sur l'expérience des Canadiens relativement à la cybercriminalité.

En 2013, **Norton** a publié une étude commandée par Symantec sur la prévalence et les coûts financiers de la cybercriminalité, fondée sur une enquête auprès des adultes qui utilisaient Internet dans 24 pays. Selon cette étude, on estime que 68 % des utilisateurs d'Internet canadiens d'âge adulte ont été victimes de cybercriminalité au cours de leur vie, tandis que 42 % l'ont été durant les 12 mois qui ont précédé l'enquête. Par ailleurs, on estime, dans cette étude, que le coût de la cybercriminalité au Canada au cours des 12 mois ayant précédé la tenue de l'enquête était d'environ 3 milliards de dollars américains (Norton 2013). Ces constatations sont corroborées par les recherches menées par le **Center for Strategic and International Studies** et commanditées par Intel Security. Selon ces recherches, qui s'appuient sur les données publics et les renseignements obtenus des représentants du gouvernement, d'experts et d'entreprises de cybersécurité, le coût annuel de la cybercriminalité au Canada correspondait à 0,17 % du produit intérieur brut (PIB) du pays (Center for Strategic and International Studies, 2014).

Ciblant les différents types de fraude par marketing de masse (télémarketing), comme les pourriels et la fraude d'identité, le **Centre antifraude du Canada** recueille des données à partir des plaintes et des appels des victimes. Il reçoit ces plaintes par téléphone à un centre d'appels national. Auparavant appelée Phonebusters, cette initiative est menée en collaboration avec la Gendarmerie royale du Canada, le Bureau de la concurrence Canada et la Police provinciale de l'Ontario et rend compte du nombre de plaintes reçues en fonction du moyen de sollicitation, notamment par Internet, au téléphone ou par la poste. En 2013, le Centre antifraude du Canada a reçu environ 43 000 plaintes de fraude par marketing de masse, représentant environ 12 000 victimes; les pertes totales d'argent signalées s'établissaient à plus de 52 millions de dollars. Selon les données, les courriels ou Internet sont les moyens de sollicitation ayant été à l'origine de 56 % des pertes totales d'argent signalées. En outre, le Centre antifraude du Canada a identifié près de 20 000 victimes de fraude d'identité en 2013, les pertes totales d'argent signalées se chiffrant à environ 11 millions de dollars (Centre d'appel antifraude du Canada, 2014).

Cyberaide.ca, exploité par un organisme caritatif connu sous le nom de Centre canadien de protection de l'enfance, reçoit et analyse de l'information sur l'exploitation sexuelle des enfants sur Internet. Ces renseignements proviennent des signalements du public faits par Internet et par téléphone relativement à des infractions telles que la pornographie juvénile, le leurre d'enfants et le trafic d'enfants. En 2013-2014, 24 911 cas d'exploitation sexuelle d'enfants sur Internet ont été signalés à Cyberaide.ca. Ces signalements ont été analysés avant d'être envoyés au service de police approprié ou à l'organisme de protection de l'enfance indiqué, lorsqu'il y avait lieu de croire qu'un acte criminel avait été commis (Cyberaide.ca, 2014).

La cyberintimidation autodéclarée

Comme pour la criminalité en général, une des limites que posent les données sur les cybercrimes déclarés par la police est le fait que toutes les infractions commises ne sont pas portées à l'attention de la police. L'Enquête sociale générale (ESG) de 2009 a permis de recueillir des renseignements sur les personnes ayant déclaré avoir été victimes sur Internet sans nécessairement avoir signalé l'incident à la police. Ces données viennent compléter celles provenant de la police parce qu'elles permettent d'estimer la prévalence de la victimisation sur Internet au Canada[14].

À l'aide des résultats de l'ESG de 2009 sur la victimisation, la section qui suit porte sur les caractéristiques des personnes qui ont déclaré avoir été victimes de cyberintimidation, ainsi que sur les mesures de protection et les précautions qu'elles ont dit prendre dans leur vie quotidienne (voir l'encadré 5).

Encadré 5
Définitions de la victimisation autodéclarée sur Internet

Les définitions suivantes sont tirées des questions posées aux Canadiens âgés de 15 ans et plus dans le cadre de l'Enquête sociale générale (ESG) de 2009. Il est important de noter que les données obtenues à partir de ces questions reposent sur les perceptions de ces personnes et ne devraient pas être comparées aux données déclarées par la police.

Cyberintimidation : Dans le cadre de l'ESG, on a demandé aux Canadiens s'ils avaient déjà reçu des messages menaçants ou agressifs, ou des courriels menaçants en utilisant l'identité de la victime ; ou s'ils avaient déjà été la cible de commentaires haineux envoyés par courriel ou messagerie instantanée, ou affichés sur des sites Internet.

Mesures de protection : Dans le cadre de l'ESG, on a demandé aux personnes de 15 ans et plus si elles avaient déjà pris l'un ou l'autre des moyens suivants pour se protéger ou protéger leurs biens contre des actes criminels au cours des 12 mois ayant précédé la tenue de l'enquête, comme : changer leurs habitudes ou leurs activités, ou encore éviter certaines personnes ou certains endroits; poser de nouvelles serrures ou des barres de sécurité; installer un système d'éclairage détecteur de mouvements; suivre un cours d'autodéfense; se procurer un chien; se procurer une arme à feu; et déménager ou changer de résidence.

Précautions prises au quotidien : L'ESG a aussi posé aux Canadiens des questions sur les précautions qu'ils prenaient au quotidien. Contrairement aux mesures de protection, les précautions prises n'ont pas de période de référence précise. Il peut s'agir de nouvelles habitudes en place depuis quelques mois ou d'habitudes établies depuis de nombreuses années. Les précautions sont les suivantes : emporter quelque chose avec soi pour donner l'alerte ou pour se défendre; vérifier qu'aucun intrus ne se trouve sur le siège arrière de sa voiture avant d'y monter lorsqu'on est seul; déterminer son trajet en fonction de sa sécurité; rester à la maison le soir par crainte de sortir seul; verrouiller les portes et les fenêtres à la maison; prendre sa voiture, un taxi ou le transport en commun plutôt que de marcher pour assurer sa sécurité personnelle.

Utilisateurs d'Internet : Aux fins du présent article, les utilisateurs d'Internet sont ceux qui ont déclaré avoir utilisé Internet au cours des 12 mois ayant précédé la tenue de l'enquête.

Les adolescents sont les plus susceptibles de déclarer être la cible de cyberintimidation

En 2009, environ 1,75 million de Canadiens de 15 ans et plus ont déclaré avoir été victimes de cyberintimidation, ce qui représentait 8 % des utilisateurs d'Internet âgés de 15 ans et plus. Près de 1 jeune[15] sur 5 (19 %) de 15 à 17 ans a indiqué avoir fait l'objet de cyberintimidation, alors que c'était le cas chez 17 % des jeunes adultes de 18 à 24 ans. Cette proportion s'établissait à 9 % chez les personnes de 25 à 34 ans, puis à 5 % ou moins chez celles de 35 ans et plus (tableau 6).

Les utilisateurs des sites de réseautage social sont proportionnellement plus nombreux à déclarer être victimes de cyberintimidation

Les sites de réseautage social tels que Facebook et MySpace sont d'importantes plateformes d'échanges sociaux. L'utilisation de telles plateformes de réseautage social est également liée à un risque plus élevé de cyberintimidation. Selon les données de l'ESG de 2009, 12 % des utilisateurs des sites de réseautage social âgés de 15 ans et plus ont déclaré avoir été victimes d'intimidation, alors que cela a été le cas de 3 % de ceux qui ne faisaient pas de réseautage social. Parmi les utilisateurs des salons de clavardage, 15 % ont mentionné avoir été victimes de cyberintimidation, soit plus du double de la proportion de ceux qui n'utilisaient pas ces forums (5 %).

Bien que l'utilisation des sites de réseautage social soit particulièrement fréquente chez les jeunes, les utilisateurs de ces sites courent constamment un plus grand risque d'être la cible de cyberintimidation, quel que soit leur âge. En effet, 19 % des utilisateurs des sites de réseautage social âgés de 18 à 24 ans ont déclaré avoir été victimes de cyberintimidation, comparativement à 9 % des personnes qui ne les utilisaient pas. Parmi les personnes de 45 à 54 ans, 8 % des utilisateurs de sites de réseautage social ont dit avoir été la cible de cyberintimidation, comparativement à 3 % de celles qui n'utilisaient pas ces sites.

Une victime de cyberintimidation sur cinq a aussi déclaré avoir fait l'objet d'un crime violent

Selon les résultats de l'ESG de 2009, la victimisation en ligne était associée à une incidence accrue de la victimisation avec violence. En 2009, 11 % des utilisateurs d'Internet âgés de 15 ans et plus qui ont déclaré avoir été victimes de cyberintimidation ont également dit avoir reçu des menaces de voies de fait et 21 % ont indiqué avoir été victimes d'au moins un crime violent au cours des 12 mois ayant précédé la tenue de l'enquête. À titre de comparaison, parmi les non-victimes de cyberintimidation, 6 % ont déclaré avoir été la cible d'au moins un crime violent. Cette différence est surtout marquée chez les jeunes. En effet, la proportion de victimes de cyberintimidation chez les jeunes de 15 à 17 ans qui ont également été victimes d'un crime violent s'établissait à 32 % par rapport à 12 % des répondants de ce groupe d'âge qui n'ont pas déclaré avoir été victimes de cyberintimidation. Parmi les personnes de 18 à 24 ans, 27 % des victimes de cyberintimidation ont dit avoir aussi fait l'objet d'un crime violent, comparativement à 12 % de celles qui n'ont pas déclaré avoir été la cible de cyberintimidation.

Les résultats de l'ESG n'indiquent pas si les auteurs présumés des crimes violents sont ceux qui commettent des actes de cyberintimidation. D'autres recherches seront nécessaires pour examiner le lien entre la victimisation sur Internet et la victimisation avec violence.

La majorité des victimes de cyberintimidation ne signalent pas l'incident à la police

Moins de 1 victime de cyberintimidation sur 10 (7 %) a signalé l'incident à la police, selon les données de l'ESG de 2009. L'incident a été signalé à la police par 8 % des femmes victimes de cyberintimidation et 5 % des hommes victimes de ce crime. Selon des recherches, les groupes plus jeunes sont moins susceptibles de signaler les incidents de victimisation à la police (Perreault et Brennan, 2010).

Des recherches antérieures ont révélé que les victimes de cyberintimidation sont plus susceptibles de bloquer les messages de l'expéditeur, de quitter le site Internet ou de signaler la situation à leur fournisseur de service Internet que de signaler l'incident à la police (Perreault, 2011).

Plus de la moitié des victimes de cyberintimidation ont indiqué prendre des mesures de protection

Dans le cadre de l'ESG de 2009, on a demandé aux répondants s'ils avaient pris des mesures de précaution pour assurer leur sécurité personnelle au cours des 12 mois ayant précédé la tenue de l'enquête. Au total, 59 % des personnes qui ont été victimes de cyberintimidation ont dit avoir pris au moins une mesure de protection (tableau 7). Le pourcentage s'élevait à 40 % chez les non-victimes de cyberintimidation[16].

Parmi les personnes ayant déclaré avoir été victimes à la fois de cyberintimidation et d'un crime violent, 3 sur 4 (75 %) avaient pris une mesure de protection, comparativement à 54 % des Canadiens qui avaient été victimes de cyberintimidation seulement. Chez les personnes qui n'avaient pas été victimes de cyberintimidation ou d'un crime violent, cette proportion s'établissait à 39 %.

Parmi les mesures de protection prises, 47 % des victimes de cyberintimidation ont mentionné qu'elles avaient changé leurs habitudes ou leurs activités, ou qu'elles évitaient certaines personnes ou certains endroits, tandis que 18 % ont dit avoir posé de nouvelles serrures ou des barres de sécurité. Chez les non-victimes de cyberintimidation, les pourcentages correspondants étaient de 28 % et de 13 % respectivement.

Les victimes de cyberintimidation ont déclarés prendre plus de précautions au quotidien

Outre les nouvelles mesures de protection indiquées à la section précédente, dans l'ESG sur la victimisation, on a posé des questions aux Canadiens sur certaines précautions qu'ils pourraient prendre dans leur vie quotidienne[17]. Les victimes de cyberintimidation ont indiqué être plus portées à prendre certaines précautions que les non-victimes. Parmi les victimes de cyberintimidation, 28 % emportaient quelque chose sur elles pour se défendre, comparativement à 15 % des non-victimes de cyberintimidation (tableau 7). Plus de la moitié (53 %) des victimes de cyberintimidation déterminaient leur trajet en fonction de leur sécurité, comparativement à 43 % des non-victimes. Parmi les victimes, 14 % ont dit rester à la maison parce qu'elles avaient peur, par rapport à 8 % des personnes qui n'avaient pas été la cible de cyberintimidation.

Les victimes de cyberintimidation qui ont également déclaré avoir fait l'objet d'au moins un crime violent étaient plus susceptibles que celles qui n'ont pas été victimes d'un crime violent de prendre plus de précautions. Parmi les victimes de cyberintimidation qui ont également été victimes d'un crime violent, 47 % prenaient au moins quatre précautions, comparativement à 32 % des personnes qui ont déclaré avoir été victimes de cyberintimidation seulement.

De façon générale, les femmes sont plus susceptibles que les hommes de prendre des précautions au quotidien. Selon les données de l'ESG, 49 % des femmes victimes de cyberintimidation ont dit prendre au moins quatre précautions, soit 12 points de pourcentage de plus que les femmes qui n'avaient pas été victimes de cyberintimidation (37 %). Chez les hommes, 20 % des victimes de cyberintimidation ont dit prendre au moins quatre mesures de sécurité, par rapport à 11 % des hommes qui n'avaient pas été victimes de ce type de crime.

Les victimes de cyberintimidation disent être plus stressées que les non-victimes

Les victimes de cyberintimidation étaient plus susceptibles de déclarer des niveaux plus élevés de stress dans leur vie quotidienne que les non-victimes. En 2009, plus du tiers (36 %) des victimes ont déclaré que leurs journées étaient assez stressantes ou extrêmement stressantes, comparativement à 24 % des personnes qui n'avaient pas été victimes de cyberintimidation.

En général, les femmes étaient plus susceptibles que les hommes de déclarer des niveaux plus élevés de stress. Quel que soit leur sexe, les victimes de cyberintimidation avaient plus tendance à indiquer que leurs journées étaient assez stressantes ou extrêmement stressantes. Il en va de même pour 39 % des femmes victimes, comparativement à 26 % des non-victimes. Parmi les hommes victimes de cyberintimidation, 32 % ont mentionné que leurs journées étaient assez stressantes ou extrêmement stressantes, alors que la proportion s'établissait à 23 % chez les non-victimes.

Résumé

Les services de police desservant 80 % de la population du Canada ont déclaré 9 084 affaires de cybercriminalité en 2012. Le type de cybercrime le plus courant était la fraude, représentant plus de la moitié (54 %) de l'ensemble des cybercrimes déclarés par la police en 2012. Les infractions liées à l'intimidation, composées des infractions comportant des menaces de violence, constituaient 20 % des cybercrimes déclarés par la police en 2012, alors que 16 % des cybercrimes comportaient une infraction cybernétique de nature sexuelle.

En 2012, un auteur présumé a été identifié dans 6 % des cybercrimes contre les biens, dans 31 % des infractions cybernétiques de nature sexuelle et dans 55 % des cybercrimes associés à des infractions liées à l'intimidation. Comparativement aux infractions liées à l'intimidation, les infractions sexuelles étaient plus souvent classées par mise en accusation (25 % par rapport à 18 %).

La majorité (76 %) des auteurs présumés identifiés par la police en 2012 étaient des hommes. Cette constatation est particulièrement marquée dans le cas des infractions de nature sexuelle, pour lesquelles les hommes représentaient 94 % des auteurs présumés identifiés par la police.

En 2012, la police a identifié 2 070 victimes d'affaires de violence comportant un cybercrime. Les femmes représentaient la majorité des victimes d'affaires de violence associées à un cybercrime (69 %), tout particulièrement lorsque ces affaires comprenaient une infraction sexuelle (84 %).

Les victimes de cybercrimes identifiées par la police ont tendance à être jeunes. En 2012, 42 % des victimes de cybercrimes déclarés par la police avaient moins de 18 ans. Presque la totalité (96 %) des victimes d'infractions sexuelles associées à un cybercrime avaient moins de 18 ans, y compris 10 % d'entre elles qui avaient moins de 12 ans.

La plupart des victimes (73 %) connaissaient l'auteur présumé. Les victimes d'infractions sexuelles comportant un cybercrime étaient moins susceptibles de connaître l'auteur présumé (57 %) que les victimes d'infractions avec violence de nature non sexuelle (77 %).

Selon les résultats de l'ESG de 2009, environ 1,75 million de personnes de 15 ans et plus ont déclaré avoir été victimes de cyberintimidation. Cela représentait 8 % des utilisateurs d'Internet âgés de 15 ans et plus. Moins de 1 victime sur 10 (7 %) de cyberintimidation a signalé l'incident à la police.

Description des enquêtes

Programme de déclaration uniforme de la criminalité

Le présent rapport s'appuie sur les données du Programme de déclaration uniforme de la criminalité fondé sur l'affaire (DUC 2). Il s'agit d'une enquête à base de microdonnées qui permet de recueillir des renseignements détaillés sur les crimes signalés à la police et confirmés par cette dernière, y compris les caractéristiques des victimes, des auteurs présumés et des affaires. Compte tenu de l'évolution des besoins en information, l'enquête a été modifiée en 2005 (version 2.2) pour que l'on

puisse recueillir des données sur les affaires criminelles liées à des crimes motivés par la haine, le crime organisé et la cybercriminalité.

Le Programme DUC 2 (version 2.2) permet de recueillir des renseignements sur les affaires mettant en cause des infractions cybernétiques. Les affaires criminelles peuvent comporter de nombreuses infractions. En 2012, il y a eu 9 084 affaires criminelles qui comportaient une infraction identifiée comme un cybercrime. Dans 8 974 (99 %) de ces cas, l'infraction cybernétique était l'infraction la plus grave dans l'affaire.

Les données sur les cybercrimes déclarés par la police représentaient les services de police desservant 80 % de la population du Canada. Puisque les données de Saint John, de Québec, de Toronto, de Calgary et de la Police provinciale de l'Ontario n'étaient pas disponibles, elles ne sont pas incluses dans la présente analyse.

Enquête sociale générale sur la victimisation

En 2009, Statistique Canada a réalisé le cycle de la victimisation de l'Enquête sociale générale (ESG) pour la cinquième fois. Les cycles précédents ont été menés en 1988, 1993, 1999 et 2004. Les objectifs de l'enquête étaient les suivants : fournir des estimations de l'expérience personnelle qu'ont les Canadiens de huit types d'infractions; examiner les facteurs de risque liés à la victimisation; examiner les taux de déclaration à la police; évaluer la nature et l'étendue de la violence conjugale; mesurer la crainte de la criminalité; et examiner les perceptions du public à l'égard de la criminalité et du système de justice pénale. Pour la première fois en 2009, l'ESG a aussi permis de recueillir des renseignements sur l'expérience des Canadiens relativement à la victimisation sur Internet, soit la fraude par Internet, la cyberintimidation et les problèmes éprouvés en faisant des achats en ligne.

La population cible comprenait toutes les personnes de 15 ans et plus résidant dans les 10 provinces canadiennes, à l'exclusion des personnes vivant en établissement à temps plein. Les ménages étaient sélectionnés au moyen d'un échantillonnage téléphonique à l'aide de la méthode de la composition aléatoire. Les ménages qui n'avaient pas de numéro de téléphone ou qui utilisaient un téléphone cellulaire seulement ont été exclus. Ensemble, ces deux groupes représentaient environ 9 % de la population cible (Enquête sur le service téléphonique résidentiel, décembre 2008). Par conséquent, la couverture pour 2009 était de 91 %. La collecte de données s'est déroulée de février à novembre 2009 inclusivement. Parmi les 31 510 ménages choisis pour faire partie de l'échantillon du cycle 23 de l'ESG, 19 422 ont fourni des réponses exploitables. Cela représente un taux de réponse de 61,6 %. Chaque personne qui a participé à l'ESG de 2009 représentait environ 1 400 personnes de 15 ans et plus dans la population canadienne.

Références

BRENNAN, Shannon. 2012. « Statistiques sur les crimes déclarés par la police au Canada, 2011 », *Juristat*, produit n° 85-002-X au catalogue de Statistique Canada.

Center for Strategic and International Studies. 2014. *Net Losses: Estimating the Global Cost of Cybercrime*, Intel Security http://www.mcafee.com/ca/resources/reports/rp-economic-impact-cybercrime2.pdf (site consulté le 8 septembre 2014).

Centre antifraude du Canada. 2014. *Rapport statistique annuel 2013*, Groupe de l'analyse du renseignement criminel du Centre antifraude du Canada https://www.antifraudcentre-centreantifraude.ca/francais/documents/Annual%202013%20CAFC%20fr.pdf https://www.cybertip.ca/app/fr/about (site consulté le 8 septembre 2014).

Centre canadien de la statistique juridique. 2013. *Manuel du Programme de déclaration uniforme de la criminalité fondé sur l'affaire*, non publié.

COTTER, Adam, et Pascale BEAUPRE. 2014. « Les infractions sexuelles commises contre les enfants et les jeunes déclarées par la police au Canada, 2012 », *Juristat*, produit n° 85-002-X au catalogue de Statistique Canada.

Cybertip.ca. 2014. *Statistiques globales* https://www.cybertip.ca/app/fr/about (site consulté le 8 septembre 2014).

Gendarmerie royale du Canada. 2014. *Cybercriminalité : survol des incidents et des enjeux au Canada*, produit n° PS64-116/2014F-PDF au catalogue http://www.rcmp-grc.gc.ca/pubs/cc-report-rapport-cc-fra2.pdf (site consulté le 8 septembre 2014).

KOWALSKI, Melanie. 2002. *Cybercriminalité : questions, sources de données et faisabilité de la collecte de données auprès de la police*, Centre canadien de la statistique juridique, produit n° 85-558-X au catalogue de Statistique Canada.

HOTTON MAHONY, Tina, et John TURNER. 2012. « Les taux de classement des affaires déclarées par la police au Canada, 2010 », *Juristat*, produit n° 85-002-X au catalogue de Statistique Canada.

Norton. 2013. *2013 Norton Report*, Symantec http://www.symantec.com/content/en/us/about/presskits/b-norton-report-2013.en_ca.pdf (site consulté le 8 septembre 2014).

NUTH, Maryke S. 2008. « Taking Advantage of New Technologies: For and Against Crime », *Computer Law and Security Review*, vol. 24, n° 5.

PERREAULT, Samuel. 2011. « Les incidents autodéclarés de victimisation sur Internet au Canada, 2009 », *Juristat*, produit n° 85-002-X au catalogue de Statistique Canada.

PERREAULT, Samuel. 2013. « Statistiques sur les crimes déclarés par la police au Canada, 2012 », *Juristat*, produit n° 85-002-X au catalogue de Statistique Canada.

PERREAULT, Samuel, et Shannon BRENNAN. 2010. « La victimisation criminelle au Canada, 2009 », *Juristat*, produit n° 85-002-X au catalogue de Statistique Canada.

SMYTH, Sara M., et Rebecca CARLETON. 2011. *Évaluation de l'ampleur de la cyberfraude : document de travail sur les méthodes potentielles et les sources de données*, document préparé pour la Division de la recherche et de la coordination nationale sur le crime organisé, Secteur de la police et de l'application de la loi, Sécurité publique Canada, n° 020, produit n° 978-1-100-97864-2 au catalogue http://publications.gc.ca/collections/collection_2012/sp-ps/PS14-4-2011-fra.pdf (site consulté le 8 septembre 2014).

Statistique Canada, 2013. « Utilisation d'Internet et du commerce électronique par les particuliers, 2012 », *Le Quotidien, 28 octobre* http://www.statcan.gc.ca/daily-quotidien/131028/dq131028a-fra.htm (site consulté le 8 septembre 2014).

Notes

1. Le Programme de déclaration uniforme de la criminalité fondé sur l'affaire (version 2.2) saisit des renseignements détaillés sur les cybercrimes signalés à la police et confirmés par celle ci. Pour obtenir plus de renseignements sur le Programme DUC (version 2.2), voir la section « Description des enquêtes ». Pour en savoir plus sur la définition des affaires de cybercriminalité, voir l'encadré 1.

2. Aux fins de l'analyse, les affaires de cybercriminalité dans lesquelles l'infraction cybernétique n'était pas une infraction au *Code criminel* sont exclues du présent rapport. Par conséquent, 4 affaires de trafic de drogues et 13 affaires liées à des infractions à d'autres lois fédérales sont exclues de l'analyse.

3. Les données sur la cybercriminalité déclarées par la police étaient disponibles pour les services de police desservant 80 % de la population du Canada. Puisque les données de Saint John, de Québec, de Toronto, de Calgary et de la Police provinciale de l'Ontario n'étaient pas disponibles, elles ne sont pas incluses dans la présente analyse. Pour en savoir plus sur la collecte des données sur la cybercriminalité déclarées par la police, voir la section « Description des enquêtes ».

4. Le calcul des taux repose sur les chiffres de population obtenus à partir du sous-ensemble de services de police ayant fourni des données sur la cybercriminalité au Programme DUC (version 2.2).

5. L'infraction appelée **« fraude »** dans le Programme DUC est un regroupement de plusieurs infractions au *Code criminel*. Une fraude est un acte criminel selon lequel un individu ou un groupe d'individus, par supercherie, mensonge ou autres moyen dolosif, frustre le public ou toute personne de quelque bien, service, argent ou valeur. Toute fraude comportant l'utilisation non autorisée d'un ordinateur ou l'utilisation d'un ordinateur ou d'Internet à des fins illégales est un cybercrime. La fraude d'identité et le vol d'identité se distinguent de la fraude dans le Programme DUC.

6. Puisque cette analyse porte uniquement sur les affaires de cybercriminalité corroborées par les services de police, elle n'est pas le reflet de tous les cas de victimisation en ligne subis par les Canadiens. Voir les autres sources des données et les estimations de la cyberfraude dans l'encadré 4.

7. Les infractions contre la personne comprennent les infractions sexuelles, les infractions liées à l'intimidation et les autres infractions avec violence. Les infractions contre la personne comprennent celles pour lesquelles les renseignements sur les victimes doivent être fournis ou sont exigés s'ils sont connus. Aux fins de la présente analyse, les infractions sexuelles comprennent les infractions de pornographie juvénile pour lesquelles les renseignements sur les victimes ne sont pas

disponibles. Pour obtenir la liste des infractions qui font partie des catégories « Infractions sexuelles » et « Infractions liées à l'intimidation », voir le tableau 1.

8. La catégorie **« Leurre d'enfants/entente ou arrangement »** dans le Programme DUC comprend deux infractions distinctes au *Code criminel* : leurre d'enfants au moyen d'un ordinateur (article 172.1) et entente ou arrangement — infraction d'ordre sexuel à l'égard d'un enfant (article 172.2). Le leurre d'enfants est une infraction mixte qui criminalise la communication avec un enfant par un moyen de télécommunication en vue de faciliter la perpétration à son égard d'une infraction d'ordre sexuel. L'entente ou l'arrangement est une infraction mixte qui criminalise le fait de s'entendre avec une personne ou de prendre un arrangement avec elle par un moyen de télécommunication pour perpétrer une infraction d'ordre sexuel à l'endroit d'un enfant. Cette infraction a été adoptée en août 2012. Pour chacune de ces infractions, la peine maximale d'emprisonnement est de 10 ans si l'infraction est punissable sur acte d'accusation et de 18 mois si l'infraction est punissable sur déclaration de culpabilité par procédure sommaire. Une peine minimale obligatoire d'un an d'emprisonnement s'applique s'il y a mise en accusation et une peine de 90 jours s'applique s'il y a déclaration de culpabilité par procédure sommaire.

9. En raison de la complexité de ces affaires de cybercriminalité, les données représentent probablement le nombre d'enquêtes actives ou closes pour l'année plutôt que le nombre total d'affaires signalées à la police. La catégorie « pornographie juvénile » dans le Programme DUC comprend les infractions prévues à l'article 163.1 du *Code criminel*, qui stipule qu'il est illégal de posséder, de produire, d'imprimer ou de distribuer de la pornographie juvénile ou encore d'y accéder. Dans les cas où la victime n'est pas identifiée, cette infraction est consignée au Programme DUC de telle sorte que l'infraction la plus grave soit la « pornographie juvénile ». Aux fins de l'analyse des affaires de cybercriminalité, ce genre d'infractions fait partie des « infractions sexuelles », qui sont regroupées sous les cybercrimes contre la personne. Dans les cas où la victime est identifiée, la police consigne l'infraction la plus grave comme une agression sexuelle, de l'exploitation sexuelle ou une autre infraction sexuelle contre un enfant; la pornographie juvénile peut alors être consignée comme une infraction secondaire.

10. Pour qu'une affaire soit classée, un auteur présumé doit être identifié et il doit y avoir suffisamment de preuves pour porter une accusation en lien avec l'affaire. Les affaires peuvent être classées soit par mise en accusation, soit sans mise en accusation. Les statistiques sur les crimes déclarés par la police montrent constamment que les infractions contre les biens sont moins susceptibles d'être classées que les infractions avec violence (Mahony et Turner, 2012).

11. L'analyse des victimes de cybercrimes déclarés par la police est fondée sur les victimes de crimes violents qui comportaient aussi une infraction cybernétique. Les victimes sont réparties selon l'infraction commise à leur égard. L'infraction commise contre la victime n'est pas nécessairement l'infraction cybernétique. Il peut y avoir plusieurs victimes associées à une affaire criminelle. Il se peut que le nombre de victimes analysées dans ce rapport soit une sous-estimation puisque les détails sur les victimes ne sont peut-être pas disponibles pour des infractions avec violence particulières, notamment le leurre d'enfants au moyen d'un ordinateur, le voyeurisme, l'extorsion, le harcèlement criminel et les menaces. Par ailleurs, puisque les renseignements sur les victimes ne sont disponibles que pour les infractions avec violence, les personnes qui étaient la cible de cybercrimes contre les biens, comme la fraude, n'ont pas été prises en compte dans l'analyse des victimes.

12. Aux fins de l'analyse des victimes d'affaires de violence associées à un cybercrime, l'infraction contre la victime a été classée comme une infraction avec violence de nature sexuelle ou une infraction avec violence de nature non sexuelle. Pour obtenir la liste des infractions qui font partie de chacune de ces catégories, voir le tableau 5. Les infractions avec violence de nature sexuelle ne comprennent pas les infractions de pornographie juvénile puisque les renseignements sur les victimes ne sont pas disponibles pour de telles infractions. Pour obtenir les explications sur la manière dont les infractions de pornographie juvénile sont déclarées au Programme DUC, voir dans la note 9.

13. La proportion de victimes visées par un étranger est peut être une sous-estimation puisque certaines victimes ne sont pas identifiées par la police.

14. Les données les plus récentes de l'Enquête sociale générale (ESG) sur la victimisation sont les résultats de 2009. Pour obtenir une analyse plus approfondie de la victimisation sur Internet autodéclarée au Canada fondée sur les données de l'ESG de 2009, voir Perreault, 2011. L'ESG sur la victimisation est réalisée tous les cinq ans, et le cycle de 2014 est actuellement en cours.

15. Selon des recherches antérieures, les enfants et les jeunes courent un plus grand risque d'être victimes de cyberintimidation. On a demandé aux répondants adultes dans le cadre de l'ESG de 2009, si l'un des enfants (âgés de 8 à 17 ans) de leur ménage avait été victime de cyberintimidation. Environ 1 adulte sur 10 vivant dans un ménage où il y avait un enfant était au courant d'un cas de cyberintimidation contre au moins un des enfants de son ménage (Perreault, 2011).

16. Ces pourcentages sont fondés sur le fait qu'une personne a été victime ou non de cyberintimidation. Il est possible que les personnes aient été victimes d'autres types de crimes.

17. Pour obtenir la liste des précautions prises au quotidien, voir le tableau 7.

Tableaux de données détaillés

Tableau 1
Cybercrimes déclarés par la police, certains services de police, 2012

Infractions cybernétiques[1]	nombre	taux pour 100 000 habitants	pourcentage du total
Total des cybercrimes contre la personne	**3,284**	**11.8**	**36.2**
Infractions sexuelles	**1,441**	**5.2**	**15.9**
Incitation à des contacts sexuels	67	0.2	0.7
Exploitation sexuelle	10	0.0	0.1
Leurre d'enfants/entente ou arrangement	543	2.0	6.0
Voyeurisme	11	0.0	0.1
Autres infractions sexuelles[2]	5	0.0	0.1
Pornographie juvénile[3]	805	2.9	8.9
Infractions liées à l'intimidation	**1,839**	**6.6**	**20.2**
Extorsion	136	0.5	1.5
Intimidation d'une personne[4]	7	0.0	0.1
Harcèlement criminel	560	2.0	6.2
Appels téléphoniques menaçants ou harcelants	377	1.4	4.2
Menaces	759	2.7	8.4
Autres infractions avec violence[5]	**4**	**0.0**	**0.0**
Total des cybercrimes contre les biens	**5,544**	**20.0**	**61.0**
Fraude	4,878	17.6	53.7
Vol d'identité	73	0.3	0.8
Fraude d'identité	421	1.5	4.6
Méfait	170	0.6	1.9
Trafic de biens volés	2	0.0	0.0
Total des autres infractions au *Code criminel*[6]	**256**	**0.9**	**2.8**
Total — ensemble des infractions au *Code criminel*	**9,084**	**32.7**	**100.0**

1. Les chiffres sont fondés sur l'infraction dans l'affaire pour laquelle un ordinateur ou Internet était la cible du crime ou l'instrument employé pour perpétrer le crime.
2. Comprend la corruption d'enfants, le fait de rendre accessible à un enfant du matériel sexuellement explicite, et la bestialité — la perpétration ou l'usage de la force.
3. En raison de la complexité de ces affaires de cybercriminalité, les données représentent probablement le nombre d'enquêtes actives ou closes pour l'année plutôt que le nombre total d'affaires signalées à la police. La catégorie « Pornographie juvénile » comprend les infractions prévues à l'article 163.1 du *Code criminel*, qui stipule qu'il est illégal de posséder, de produire, d'imprimer ou de distribuer de la pornographie juvénile ou encore d'y accéder. Dans les cas où la victime n'est pas identifiée, cette infraction est consignée au Programme de déclaration uniforme de la criminalité de telle sorte que l'infraction la plus grave soit la « pornographie juvénile ». Aux fins de la présente analyse, ce genre d'infractions fait partie des infractions sexuelles, qui sont regroupées sous les cybercrimes contre la personne. Dans les cas où la victime est identifiée, la police consigne l'infraction la plus grave comme une agression sexuelle, de l'exploitation sexuelle ou une autre infraction sexuelle contre un enfant; la pornographie juvénile peut alors être consignée comme une infraction secondaire.
4. Comprend l'intimidation d'une personne associée au système judiciaire ou d'un journaliste et l'intimidation d'une personne qui n'est pas associée au système judiciaire.
5. Comprend la traite de personnes et d'autres infractions avec violence.
6. Comprend des infractions telles que la corruption des mœurs, les actions indécentes, les infractions contre la personne et la réputation, le défaut de se conformer à une ordonnance et le manquement aux conditions de la probation.

Note : Les renseignements qui figurent dans le présent tableau reflètent les données déclarées par les services de police desservant 80 % de la population du Canada. Puisque les données de Saint John, de Québec, de Toronto, de Calgary et de la Police provinciale de l'Ontario n'étaient pas disponibles, elles ne sont pas incluses dans la présente analyse.

Source : Statistique Canada, Centre canadien de la statistique juridique, Programme de déclaration uniforme de la criminalité fondé sur l'affaire.

Tableau 2
Cybercrimes déclarés par la police, selon l'état de classement des affaires, certains services de police, 2012

Infractions cybernétiques[1]	Affaires classées par mise en accusation		Affaires classées sans mise en accusation		Affaires non classées		Total
	nombre	pourcentage	nombre	pourcentage	nombre	pourcentage	nombre
Total des cybercrimes contre la personne	**697**	**21,2**	**762**	**23,2**	**1 825**	**55,6**	**3 284**
Infractions sexuelles	**357**	**24,8**	**92**	**6,4**	**992**	**68,8**	**1 441**
Incitation à des contacts sexuels	53	79,1	2	3,0	12	17,9	67
Exploitation sexuelle	5	50,0	2	20,0	3	30,0	10
Leurre d'enfants/entente ou arrangement	146	26,9	41	7,6	356	65,6	543
Voyeurisme	8	72,7	2	18,2	1	9,1	11
Autres infractions sexuelles[2]	1	20,0	0	0,0	4	80,0	5
Pornographie juvénile[3]	144	17,9	45	5,6	616	76,5	805
Infractions liées à l'intimidation	**339**	**18,4**	**667**	**36,3**	**833**	**45,3**	**1 839**
Extorsion	23	16,9	14	10,3	99	72,8	136
Intimidation d'une personne[4]	1	14,3	1	14,3	5	71,4	7
Harcèlement criminel	200	35,7	193	34,5	167	29,8	560
Appels téléphoniques menaçants ou harcelants	9	2,4	154	40,8	214	56,8	377
Menaces	106	14,0	305	40,2	348	45,8	759
Autres infractions avec violence[5]	**1**	**25,0**	**3**	**75,0**	**0**	**0,0**	**4**
Total des cybercrimes contre les biens	**144**	**2,6**	**212**	**3,8**	**5 188**	**93,6**	**5 544**
Fraude	126	2,6	115	2,4	4 637	95,1	4 878
Vol d'identité	0	0,0	2	2,7	71	97,3	73
Fraude d'identité	8	1,9	71	16,9	342	81,2	421
Méfait	8	4,7	24	14,1	138	81,2	170
Trafic de biens volés	2	100,0	0	0,0	0	0,0	2
Total des autres infractions au *Code criminel*[6]	**66**	**25,8**	**49**	**19,1**	**141**	**55,1**	**256**
Total — ensemble des infractions au *Code criminel*	**907**	**10,0**	**1 023**	**11,3**	**7 154**	**78,8**	**9 084**

1. Les chiffres sont fondés sur l'infraction dans l'affaire pour laquelle un ordinateur ou Internet était la cible du crime ou l'instrument employé pour perpétrer le crime. Pour qu'une affaire soit classée, un auteur présumé doit être identifié et il doit y avoir suffisamment de preuves pour porter une accusation en lien avec l'affaire. Les affaires peuvent être classées soit par mise en accusation, soit par d'autres moyens (p. ex. sans mise en accusation).
2. Comprend la corruption d'enfants, le fait de rendre accessible à un enfant du matériel sexuellement explicite, et la bestialité — la perpétration ou l'usage de la force.
3. En raison de la complexité de ces affaires de cybercriminalité, les données représentent probablement le nombre d'enquêtes actives ou closes pour l'année plutôt que le nombre total d'affaires signalées à la police. La catégorie « Pornographie juvénile » comprend les infractions prévues à l'article 163.1 du *Code criminel*, qui stipule qu'il est illégal de posséder, de produire, d'imprimer ou de distribuer de la pornographie juvénile ou encore d'y accéder. Dans les cas où la victime n'est pas identifiée, cette infraction est consignée au Programme de déclaration uniforme de la criminalité de telle sorte que l'infraction la plus grave soit la « pornographie juvénile ». Aux fins de la présente analyse, ce genre d'infractions fait partie des infractions sexuelles, qui sont regroupées sous les cybercrimes contre la personne. Dans les cas où la victime est identifiée, la police consigne l'infraction la plus grave comme une agression sexuelle, de l'exploitation sexuelle ou une autre infraction sexuelle contre un enfant; la pornographie juvénile peut alors être consignée comme une infraction secondaire.
4. Comprend l'intimidation d'une personne associée au système judiciaire ou d'un journaliste et l'intimidation d'une personne qui n'est pas associée au système judiciaire.
5. Comprend la traite de personnes et d'autres infractions avec violence.
6. Comprend des infractions telles que la corruption des mœurs, les actions indécentes, les infractions contre la personne et la réputation, le défaut de se conformer à une ordonnance et le manquement aux conditions de la probation.

Note : Les renseignements qui figurent dans le présent tableau reflètent les données déclarées par les services de police desservant 80 % de la population du Canada. Puisque les données de Saint John, de Québec, de Toronto, de Calgary et de la Police provinciale de l'Ontario n'étaient pas disponibles, elles ne sont pas incluses dans la présente analyse.

Source : Statistique Canada, Centre canadien de la statistique juridique, Programme de déclaration uniforme de la criminalité fondé sur l'affaire.

Tableau 3
Caractéristiques des auteurs présumés de cybercrimes déclarés par la police, selon l'infraction cybernétique, certains services de police, 2012

Données démographiques[1, 2]	Total des cybercrimes contre la personne[3]		Infractions sexuelles[4]		Infractions liées à l'intimidation		Total des cybercrimes contre les biens[5]		Total des autres infractions au *Code criminel*[6]		Total — ensemble des infractions au *Code criminel*	
	nombre	%	nombre	%	nombre	%	nombre	%	nombre	%	nombre	%
Sexe												
Femme	367	23,5	29	6,1	333	30,9	99	26,6	29	24,8	495	24,1
Homme	1 195	76,5	450	93,9	743	69,1	273	73,4	88	75,2	1 556	75,9
Total	**1 562**	**100**	**479**	**100**	**1 076**	**100**	**372**	**100**	**117**	**100**	**2 051**	**100**
Âge												
Moins de 12 ans	12	0,8	1	0,2	11	1,0	1	0,3	0	0,0	13	0,6
12 à 17 ans	371	23,8	75	15,7	290	27,0	35	9,4	18	15,4	424	20,7
18 à 24 ans	324	20,7	90	18,8	234	21,7	90	24,2	18	15,4	432	21,1
25 à 34 ans	335	21,4	107	22,3	227	21,1	154	41,4	36	30,8	525	25,6
35 à 44 ans	262	16,8	84	17,5	178	16,5	61	16,4	29	24,8	352	17,2
45 à 54 ans	178	11,4	76	15,9	102	9,5	23	6,2	12	10,3	213	10,4
55 ans et plus	80	5,1	46	9,6	34	3,2	8	2,2	4	3,4	92	4,5
Total	**1 562**	**100**	**479**	**100**	**1 076**	**100**	**372**	**100**	**117**	**100**	**2 051**	**100**

1. Le nombre d'auteurs présumés est fondé sur l'infraction cybernétique dans l'affaire.
2. Les enregistrements relatifs aux auteurs présumés sont exclus lorsque l'âge ou le sexe est inconnu.
3. Comprend les infractions sexuelles contre la personne, les infractions de pornographie juvénile, les infractions liées à l'intimidation comportant des menaces de violence, et d'autres infractions avec violence.
4. Comprend les infractions sexuelles contre la personne et les infractions de pornographie juvénile.
5. Comprend la fraude, le vol d'identité, la fraude d'identité, le méfait et le trafic de biens volés.
6. Comprend des infractions telles que la corruption des mœurs, les actions indécentes, les infractions contre la personne et la réputation, le défaut de se conformer à une ordonnance et le manquement aux conditions de la probation.

Note : Les renseignements qui figurent dans le présent tableau reflètent les données déclarées par les services de police desservant 80 % de la population du Canada. Puisque les données de Saint John, de Québec, de Toronto, de Calgary et de la Police provinciale de l'Ontario n'étaient pas disponibles, elles ne sont pas incluses dans la présente analyse.

Source : Statistique Canada, Centre canadien de la statistique juridique, Programme de déclaration uniforme de la criminalité fondé sur l'affaire.

Tableau 4
Caractéristiques des victimes de cybercrimes déclarés par la police, selon l'infraction commise contre la victime, certains services de police, 2012

Données démographiques[1,2]	Total des infractions avec violence		Infractions sexuelles[3]		Infractions avec violence de nature non sexuelle[4]	
	nombre	pourcentage	nombre	pourcentage	nombre	pourcentage
Sexe						
Femme	1 432	69,2	394,0	84,2	1 038	64,8
Homme	638	30,8	74,0	15,8	564	35,2
Total	**2 070**	**100**	**468**	**100**	**1 602**	**100**
Âge						
Moins de 12 ans	82	4,0	49	10,5	33	2,1
12 à 17 ans	785	37,9	401	85,7	384	24,0
18 à 24 ans	355	17,1	7	1,5	348	21,7
25 à 34 ans	317	15,3	7	1,5	310	19,4
35 à 44 ans	275	13,3	4	0,9	271	16,9
45 à 54 ans	167	8,1	0	0,0	167	10,4
55 ans et plus	89	4,3	0	0,0	89	5,6
Total	**2 070**	**100**	**468**	**100**	**1 602**	**100**

1. Les chiffres sont fondés sur l'infraction commise contre la victime, qui n'est pas nécessairement l'infraction cybernétique dans l'affaire.
2. Les enregistrements relatifs aux victimes sont exclus lorsque l'âge ou le sexe est inconnu.
3. Comprend les agressions sexuelles, les contacts sexuels, l'incitation à des contacts sexuels, le leurre d'enfants au moyen d'un ordinateur et d'autres infractions sexuelles contre la personne.
4. Comprend les voies de fait, l'extorsion, le harcèlement criminel, appels téléphoniques menaçants ou harcelants, les menaces et d'autres infractions avec violence de nature non sexuelle.

Note : Les renseignements qui figurent dans le présent tableau reflètent les données déclarées par les services de police desservant 80 % de la population du Canada. Puisque les données de Saint John, de Québec, de Toronto, de Calgary et de la Police provinciale de l'Ontario n'étaient pas disponibles, elles ne sont pas incluses dans la présente analyse.

Source : Statistique Canada, Centre canadien de la statistique juridique, Programme de déclaration uniforme de la criminalité fondé sur l'affaire.

Tableau 5
Victimes d'infractions avec violence liées à un cybercrime, affaires déclarées par la police, selon le lien de l'auteur présumé avec la victime, certains services de police, 2012

	Lien de l'auteur présumé avec la victime										
	Partenaire intime[3]		Membre de la famille		Ami ou connaissance[4]		Étranger		Lien inconnu[5]		Total
Infractions contre la victime[1,2]	nombre	%	nombre	%	nombre	%	nombre	%	nombre	%	nombre
Total des crimes violents	**448**	**23.7**	**90**	**4.8**	**843**	**44.5**	**512**	**27.0**	**177**	**...**	**2,070**
Infractions sexuelles	**35**	**8.7**	**15**	**3.7**	**181**	**44.9**	**172**	**42.7**	**65**	**...**	**468**
Agression sexuelle armée ou causant des lésions corporelles (niveau 2)	0	0.0	0	0.0	1	100.0	0	0.0	0	...	1
Agression sexuelle (niveau 1)	18	29.5	8	13.1	32	52.5	3	4.9	6	...	67
Contacts sexuels	4	21.1	3	15.8	12	63.2	0	0.0	0	...	19
Incitation à des contacts sexuels	1	2.1	1	2.1	24	51.1	21	44.7	1	...	48
Exploitation sexuelle	1	11.1	0	0.0	7	77.8	1	11.1	1	...	10
Leurre d'enfants/entente ou arrangement	10	3.9	3	1.2	101	39.5	142	55.5	56	...	312
Voyeurisme	1	14.3	0	0.0	4	57.1	2	28.6	0	...	7
Autres infractions sexuelles[6]	0	0.0	0	0.0	0	0.0	3	100.0	1	...	4
Infractions avec violence de nature non sexuelle	**413**	**27.7**	**75**	**5.0**	**662**	**44.4**	**340**	**22.8**	**112**	**...**	**1,602**
Voies de fait graves (niveau 3)	1	50.0	0	0.0	1	50.0	0	0.0	0	...	2
Voies de fait armées ou causant des lésions corporelles (niveau 2)	7	70.0	0	0.0	1	10.0	2	20.0	1	...	11
Voies de fait simples (niveau 1)	8	47.1	0	0.0	8	47.1	1	5.9	0	...	17
Extorsion	16	18.0	1	1.1	19	21.3	53	59.6	14	...	103
Intimidation d'une personne[7]	2	25.0	0	0.0	3	37.5	3	37.5	0	...	8
Harcèlement criminel	213	47.3	21	4.7	169	37.6	47	10.4	23	...	473
Appels téléphoniques menaçants ou harcelants	76	26.4	8	2.8	128	44.4	76	26.4	14	...	302
Menaces	88	14.3	42	6.8	328	53.4	156	25.4	59	...	673
Autres infractions avec violence[8]	2	16.7	3	25.0	5	41.7	2	16.7	1	...	13

... n'ayant pas lieu de figurer
1. Les chiffres sont fondés sur l'infraction commise contre la victime, qui n'est pas nécessairement l'infraction cybernétique dans l'affaire.
2. Les enregistrements relatifs aux victimes sont exclus lorsque l'âge ou le sexe est inconnu.
3. Comprend les conjoints actuels ou anciens, les partenaires amoureux actuels ou anciens, et les autres partenaires intimes.
4. Comprend les amis, les simples connaissances, les voisins, les relations d'affaires, les relations criminelles et les symboles d'autorité.
5. Les liens inconnus sont exclus du calcul des pourcentages.
6. Comprend la corruption d'enfants, le fait de rendre accessible à un enfant du matériel sexuellement explicite, et la bestialité — la perpétration ou l'usage de la force.
7. Comprend l'intimidation d'une personne associée au système judiciaire ou d'un journaliste et l'intimidation d'une personne qui n'est pas associée au système judiciaire.
8. Comprend l'enlèvement ou la séquestration, le rapt, la traite de personnes, le vol qualifié, et d'autres infractions avec violence.
Note : Les renseignements qui figurent dans le présent tableau reflètent les données déclarées par les services de police desservant 80 % de la population du Canada. Puisque les données de Saint John, de Québec, de Toronto, de Calgary et de la Police provinciale de l'Ontario n'étaient pas disponibles, elles ne sont pas incluses dans la présente analyse.
Source : Statistique Canada, Centre canadien de la statistique juridique, Programme de déclaration uniforme de la criminalité fondé sur l'affaire.

Tableau 6
Victimes autodéclarées de cyberintimidation, selon le sexe et l'âge de la victime, Canada, 2009

Données démographiques	Victimes de cyberintimidation	
	nombre (en milliers)	pourcentage
Sexe		
Femme†	899	8
Homme	866	8
Groupe d'âge		
15 à 17 ans†	270	19
18 à 24 ans	527	17
25 à 34 ans	388	9*
35 à 44 ans	228	5*
45 à 54 ans	221	5*
55 ans et plus	130	3*
Incidents signalés à la police	116	7
Total	**1 765**	**8**

† groupe de référence
* valeur significativement différente de la catégorie de référence ($p < 0,05$)
Note : Comprend les répondants de 15 ans et plus. On a demandé aux répondants s'ils avaient déjà été victimes de cyberintimidation. Par conséquent, aucune période n'est associée à la cyberintimidation. Le calcul des pourcentages est fondé sur tous les Canadiens qui ont utilisé Internet au moins une fois au cours des 12 mois ayant précédé la tenue de l'enquête.
Source : Statistique Canada, Enquête sociale générale de 2009.

Tableau 7
Victimes autodéclarées de cyberintimidation, selon les mesures de protection et les précautions prises au quotidien, Canada, 2009

	Victimes de cyberintimidation, selon qu'elles ont ou non été également victimes d'un crime violent			
	Victimes de cyberintimidation seulement	Victimes de cyberintimidation et d'un crime violent	Non-victimes de cyberintimidation, mais victimes d'un crime violent	Non-victimes de cyberintimidation ou d'un crime violent†
Mesures de sécurité prises	pourcentage			
Au moins une mesure de protection a été prise au cours des 12 mois précédents	54*	75*	64*	39
Nouvelle mesure de protection prise au cours des 12 mois précédents				
Changer ses habitudes ou ses activités, ou encore éviter certaines personnes ou certains endroits	42*	66*	50*	26
Poser de nouvelles serrures ou des barres de sécurité	15	30*	24*	13
Installer un système d'alarme ou un système d'éclairage détecteur de mouvements	13	13[E]	13*	10
Suivre un cours d'autodéfense	5*[E]	10*[E]	8*	2
Se procurer un chien	4[E]	8*[E]	5*	2
Se procurer une arme à feu	F	F	F	0
Déménager ou changer de résidence	2[E]	6*[E]	4*[E]	1
Précaution prise au quotidien				
Emporter quelque chose avec soi pour donner l'alerte ou pour se défendre	25*	39*	30*	13
Vérifier qu'aucun intrus ne se trouve sur le siège arrière de sa voiture avant d'y monter lorsqu'on est seul	44	48	46*	40
Déterminer son trajet en fonction de sa sécurité	51*	60*	51*	43
Rester à la maison le soir par crainte de sortir seul	12	20*[E]	11	8
Verrouiller les portes et les fenêtres à la maison	85	87	85	85
Prendre sa voiture, un taxi ou le transport en commun plutôt que de marcher pour assurer sa sécurité personnelle	36*	54*	40*	31
Autres mesures de sécurité	16	27*[E]	21*	14
	nombre (en milliers)			
Total	**1 386**	**378**	**1 331**	**19 720**

Voir les notes à la fin du tableau.

Tableau 7 suite
Victimes autodéclarées de cyberintimidation, selon les mesures de protection et les précautions prises au quotidien, Canada, 2009

	Total des victimes et non-victimes de cyberintimidation	
	Victimes de cyberintimidation	Non-victimes de cyberintimidation†
Mesures de sécurité prises	pourcentage	
Au moins une mesure de protection a été prise au cours des 12 mois précédents	59*	40
Nouvelle mesure de protection prise au cours des 12 mois précédents		
Changer ses habitudes ou ses activités, ou encore éviter certaines personnes ou certains endroits	47*	28
Poser de nouvelles serrures ou des barres de sécurité	18*	13
Installer un système d'alarme ou un système d'éclairage détecteur de mouvements	13	11
Suivre un cours d'autodéfense	6*	3
Se procurer un chien	5E*	3
Se procurer une arme à feu	F	0
Déménager ou changer de résidence	3E*	1
Précaution prise au quotidien		
Emporter quelque chose avec soi pour donner l'alerte ou pour se défendre	28*	15
Vérifier qu'aucun intrus ne se trouve sur le siège arrière de sa voiture avant d'y monter lorsqu'on est seul	45*	40
Déterminer son trajet en fonction de sa sécurité	53*	43
Rester à la maison le soir par crainte de sortir seul	14*	8
Verrouiller les portes et les fenêtres à la maison	86	85
Prendre sa voiture, un taxi ou le transport en commun plutôt que de marcher pour assurer sa sécurité personnelle	40*	31
Autres mesures de sécurité	19*	14
	nombre (en milliers)	
Total	**1 765**	**21 051**

E à utiliser avec prudence
F trop peu fiable pour être publié
† groupe de référence
* valeur significativement différente de la catégorie de référence ($p < 0,05$)
Note : Comprend les répondants de 15 ans et plus. Le calcul des pourcentage est fondé sur tous les Canadiens qui ont utilisé Internet au moins une fois au cours des 12 mois ayant précédé la tenue de l'enquête. On a demandé aux répondants s'ils avaient déjà été victimes de cyberintimidation. Par conséquent, aucune période n'est associée à la cyberintimidation. On a demandé aux répondants s'ils avaient pris des mesures de sécurité au quotidien pendant une période indéterminée. Par conséquent, les précautions peuvent être nouvelles ou habituelles.
Source : Statistique Canada, Enquête sociale générale de 2009.